CLAIMS

1. A method of anti-virus processing an email having an executable attachment comprising the steps, executed by a machine, of:

a) extracting structural elements from the email;

b) examining the executable attachments for code, data or encoded data that could have created the structural elements extracted earlier; and

c) signalling that the attachment is possibly viral or not on the basis of the extent to which the examining step b) finds evidence that the structural elements have been created by that attachment.

2. .A method according to claim 1, wherein the structural elements are categorised and the step c) includes assigning a numeric score for each element which could have been created by that attachment, and signalling that the attachment is possibly viral or not on the basis of an overall score.

3. A method according to claim 2, wherein the scores are weighted according to category.

4. A method according to any one of the preceding claims, wherein the signalling step c) takes account of factors including any or all of the following attributes of the email:

standard MIME headers;
unusual MIME headers;
deviations from RFC standards;
unusual constructs;
number of attachments;
type of attachments;
encoding method used for attachments;
text content of the email; and
HTML or XHTML content of the email.

5. A method according to any one of claims 1 to 4 wherein the step a) includes extracting the structural elements as strings, the step b) includes examining the attachments

for matches of those strings and the step c) signals the attachment as possibly viral or not on the basis of the extent to which the examining step b) finds occurrences of the strings in the attachment.

6. A system for anti-virus processing an email having an executable attachment comprising the following means, implemented by a machine:

a) means for extracting structural elements from the email;

b) means for examining the executable attachments for code, data or encoded data that could have created the structural elements extracted earlier; and

c) means for signalling that the attachment is possibly viral or not on the basis of the extent to which the examining step b) finds evidence that the structural elements have been created by that attachment.

7. A system according to claim 6, wherein the structural elements are categorised and the means c) includes means for assigning a numeric score for each element which could have been created by that attachment, and signalling that the attachment is possibly viral or not on the basis of an overall score.

8. A system according to claim 7, wherein the scores are weighted according to category.

9. A system according to any one of claims 6 to 8, wherein the signalling step c) takes account of factors including any or all of the following attributes of the email:

standard MIME headers;
unusual MIME headers;
deviations from RFC standards;
unusual constructs;
number of attachments;
type of attachments;
encoding method used for attachments;
text content of the email; and
HTML or XHTML content of the email.

10. A system according to any one of claims 6 to 9 wherein the means a) includes extracting the structural elements as strings, the means b) includes examining the attachments for matches of those strings and the means c) signals the attachment as possibly viral or not on the basis of the extent to which the examining means b) finds occurrences of the strings in the attachment.